Desarrollo Seguro

Lección 2: OWASP TOP 10

eip ESCUELA INTERNACIONAL POSGRADOS

Indice

Introducción

En esta lección se han visto y explicado los 10 tipos de ataque mas comunes según el OWASP Top 10 y en la practica se pretende, dado un código, identificar todos los puntos de ataque posibles y explicar razonadamente porque se identifica ese punto.

Puntos de ataque hallados

OWASP 10: Registro y monitoreo insuficientes.

La vulnerabilidad mas evidente es el punto 10 del OWASP ya que la victima del ataque no se ha dado cuenta del mismo hasta que ha sido informada por el propio atacante.

OWASP 1: Inyección

El siguiente punto de ataque es el punto 1 del OWASP, inyección de código. Este tipo de ataques se caracterizan por realizar inyecciones de código malicioso con la finalidad de obtener información de el y como bien se detalla en el enunciado, el atacante fue capaz de obtener varios expedientes médicos, causa directa de esta vulnerabilidad.

OWASP 6: Configuración de seguridad incorrecta

Esta vulnerabilidad viene dada por la falta de autenticación a la hora de realizar una consulta a una base SQL, si el programa pidiera autenticación para realizar la consulta, por mucho que la inyección sea posible, no se obtendría información alguna ya que no se tiene la clave de acceso a la base de datos.

OWASP 3: Exposición de Datos Sensibles

Además de lo mencionado, cabe destacar otro problema; la falta de encriptación en la información, si la información del servidor estuviera encriptada de forma que fuera necesaria una clave de acceso para leer la información, el resultado obtenido por el atacante seria inútil ya que el fichero sería ilegible.